TOP 10 QUESTIONS ABOUT AGILESCAN

WHAT IS AGILESCAN?

AgileScan is a unique security solution that quickly and easily generates an inventory of cryptographic algorithms and certificates found in software and systems across your infrastructure. It identifies cryptographic risks, weaknesses, and vulnerabilities, and can accelerate your compliance goals and increase your post-quantum readiness.

WHAT CAN AGILESCAN FIND ON YOUR NETWORK?

The network component of AgileScan scans every port on target IP addresses and finds TLS server ports, as well as primary certificates and cipher suite lists presented by each port. It can also consume NetFlow to find new TLS ports on their first use, alerting you to new use of cryptography.

WHAT CAN AGILESCAN FIND ON YOUR HOSTS?

The host-based AgileScan agent is capable of analyzing the host's entire file system (or portions you specify) to find certificates, keys, binaries, and other files that implement cryptography, or make calls to cryptographic libraries. It can find outdated, weak, or vulnerable use of cryptography you weren't aware existed on the host.

WHAT ELSE CAN THE AGILESCAN AGENT FIND ON HOSTS?

The AgileScan agent can find items such as block and stream ciphers, hash functions, public key cryptography, software-based and hardware-based random number generators, certificates (including X509 and others), public and private keys, key exchange protocols, elliptic curves, cryptographic hardware drivers, including Hardware Security Modules (HSMs), and many other cryptographic artifacts.

WHAT TYPES OF HOST DEVICES DOES AGILESCAN SUPPORT?

The AgileScan agent is a lightweight, easy-to-deploy product that currently supports Windows, Mac OS X, and Linux hosts. Installation is simple and quick, and a scan can be initiated within minutes of download.

WILL MY SYSTEMS NOTICE ANY PERFORMANCE ISSUES USING AGILESCAN?

The AgileScan agent is designed to provide minimal impact on your system resources and under normal operation your other applications and processes running should not be affected. AgileScan provides you the ability to customize performance features such as number of threads used, packets per second, number of concurrent scans, specified scheduled scan window times, how often a scan should run, and how much time should pass between scans.

WHAT OTHER CUSTOMIZATION OPTIONS ARE THERE?

No two environments are identical. AgileScan is flexible enough to adapt to your unique needs. If you only want to scan specific host addresses or you want to scan complete subnets but exclude a small number of host addresses, AgileScan allows you the ability to target the systems you care the most about.

WHAT IF I NEED TO KNOW ABOUT CRYPTO USE THAT'S SPECIFIC TO MY ORGANIZATION?

In some highly regulated environments, you may not be able to use the "latest and greatest" cryptography available. For example, TLS 1.2 may be mandated for use, and not TLS 1.3. You may need to categorize use of TLS 1.3 in your environment as high risk or inappropriate. AgileScan allows you to customize the severity of crypto threats in a fashion that is relevant to you and your organization, alerting you to the use of crypto that is not yet approved for use in your industry.

WHAT SORT OF REPORTING DOES AGILESCAN OFFER?

AgileScan's reporting feature is robust and offers many different ways to present information to your stakeholders. AgileScan provides top-level overviews in PDF form intended for executives or decision-makers in an easy to digest form. Detailed reports are available in PDF, Word, and Excel. Those detailed reports provide a wealth of very specific information for your operational or technical practitioners in order to plan status updates, information to support audit efforts, migration paths, or remediation efforts.

WHAT SHOULD I DO IF I WANT TO LEARN MORE?

If you'd like to learn more about AgileScan or see what lights it can shine on the use of cryptography in your organization, **info@infosecglobal.com**.